AMENDED IN SENATE SEPTEMBER 3, 2015

AMENDED IN SENATE JUNE 23, 2015

AMENDED IN SENATE JUNE 15, 2015

AMENDED IN ASSEMBLY APRIL 6, 2015

CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

ASSEMBLY BILL No. 670

Introduced by Assembly Member Irwin

February 25, 2015

An act to amend Section 11549.3 of the Government Code, relating to technology.

LEGISLATIVE COUNSEL'S DIGEST

AB 670, as amended, Irwin. Information technology security.

(1) Existing law establishes, within the Government Operations Agency, the Department of Technology under the supervision of the Director of Technology, who is also known as the State Chief Information Officer. The department is generally responsible for the approval and oversight of information technology projects by, among other things, consulting with state agencies during initial project planning to ensure that project proposals are based on well-defined programmatic needs.

Existing law establishes, within the department, the Office of Information Security under the supervision of the Chief of the Office of Information Security. Existing law sets forth the authority of the office, including, but not limited to, the authority to conduct, or require to be conducted, an independent security assessment of any state agency,

department, or ~~office~~ *office,* the cost of which is to be funded by the state agency, department, or office being assessed.

~~This bill would, instead, impose a duty on the office to require it to conduct, or require to be conducted, an independent security assessment of every state agency, department, or office at least once every 2 years and would maintain the requirement that the state agency, department, or office being assessed fund the costs of the independent security assessment. This bill would require an independent security assessment to include specific components, to the extent practicable, and authorize the department to require a state agency, department, or office not in compliance with any recommendation made in the independent security assessment to redirect its available and authorized funds to pay the costs of complying with the recommendation.~~

~~This bill would require the results of an independent security assessment to be available only to the state agency, department, or office that was assessed. This bill would restrict the transmission or communication of the results of an independent security assessment and any related information to state government employees and state contractors who have been approved as necessary to receive this information in order to perform the assessment. The bill would require the department to adopt standards, to be included within the State Administrative Manual, setting forth the manner for the aggregate of the results of an independent security assessment to be transmitted to the department.~~

~~This bill would require the results of an independent security assessment, the aggregate of the results of an independent security assessment transmitted to the department, and any related information to be subject to all disclosure and confidentiality provisions pursuant to any state law, including, but not limited to, the California Public Records Act, including provisions of the act that exclude from the disclosure requirements, certain security records that reveal the vulnerabilities of an information technology system. This bill would require data produced during the creation of an independent security assessment to be destroyed within 1 year of its date of creation, unless the Office of Emergency Services determines that retention for a longer period of time is necessary for state security.~~

This bill would additionally require the office, in consultation with the Office of Emergency Services, to require no fewer than 35 independent security assessments of state entities each year and determine basic standards of services to be performed as part of an

independent security assessment. The bill would require the state agency, department, or office being assessed to fund the costs of its independent security assessment. The bill would require the office and the Office of Emergency Services to receive the complete results of an independent security assessment. This bill would prohibit, during the process of conducting an independent security assessment, the disclosure of information and records concerning the independent security assessment, except that the information and records would be authorized to be transmitted to state employees and state contractors with specific duties relating to the independent security assessment. The bill would require the disclosure of the results of a completed independent security assessment under state law.

This bill would require the office, in consultation with the Office of Emergency Services, to rank state entities on an information security risk index, as specified. The bill would require the office to report to the Department of Technology and the Office of Emergency Services any state entity found noncompliant with information security requirements. The bill would further require the office to notify the Office of Emergency Services, Department of the California Highway Patrol, and the Department of Justice of any criminal or alleged criminal cyber activity affecting any state entity or critical infrastructure of state government. The bill would authorize the office to conduct or require to be conducted an audit of information security to ensure program compliance, the cost of which to be funded by the state agency, department, or office being audited.

This bill would ~~also~~ authorize the Military Department to perform an independent security assessment as described above. ~~This bill would authorize the Military Department to mitigate the impact of a cyber attack or assist a law enforcement investigation into cyber security upon the request of the Office of Emergency Services, a state law enforcement agency, or a state agency, department, or office. This bill would further authorize the Military Department to perform a cyber security assessment or respond to a cyber security incident impacting state infrastructure upon the request of the Office of Emergency Services.~~

This bill would require state entities, as defined, rather than certain information security officers, to comply with policies and procedures issued by the office. The bill would also make technical, nonsubstantive changes.

(2) Existing law requires that a statute that limits the public's right of access to the meetings of public bodies or the writings of public

officials and agencies be adopted with findings to demonstrate the interest protected by the limitation and the need for protecting that interest.

This bill would limit access to ~~the results~~ *information and records* of an *ongoing* independent security assessment ~~and related records~~ and would make findings to demonstrate the interest protected by the limitation and the need for protecting that interest.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 11549.3 of the Government Code is amended to read:

11549.3. (a) The ~~director~~ *chief* shall establish an information security program. ~~The office shall report to the Department of Technology any state agency found to be noncompliant with information security program requirements.~~ The program responsibilities include, but are not limited to, all of the following:

(1) The creation, updating, and publishing of information security and privacy policies, standards, and procedures for state agencies in the State Administrative Manual.

(2) The creation, issuance, and maintenance of policies, standards, and procedures directing state agencies to effectively manage security and risk for both of the following:

(A) Information technology, which includes, but is not limited to, all electronic technology systems and services, automated information handling, system design and analysis, conversion of data, computer programming, information storage and retrieval, telecommunications, requisite system controls, simulation, electronic commerce, and all related interactions between people and machines.

(B) Information that is identified as mission critical, confidential, sensitive, or personal, as defined and published by the ~~Office of Information Security.~~ *office.*

(3) The creation, issuance, and maintenance of policies, standards, and procedures directing state agencies for the collection, tracking, and reporting of information regarding security and privacy incidents.

(4) The creation, issuance, and maintenance of policies, standards, and procedures directing state agencies in the development, maintenance, testing, and filing of each *state* agency's disaster recovery plan.

(5) Coordination of the activities of *state* agency information security officers, for purposes of integrating statewide security initiatives and ensuring compliance with information security and privacy policies and standards.

(6) Promotion and enhancement of the state agencies' risk management and privacy programs through education, awareness, collaboration, and consultation.

(7) Representing the state before the federal government, other state agencies, local government entities, and private industry on issues that have statewide impact on information security and privacy.

(b) ~~An information security officer appointed pursuant to~~ *All state entities defined in* Section 11546.1 shall implement the policies and procedures issued by the ~~Office of Information Security,~~ *office,* including, but not limited to, performing both of the following duties:

(1) Comply with the information security and privacy policies, standards, and procedures issued pursuant to this chapter by the ~~Office of Information Security.~~ *office.*

(2) Comply with filing requirements and incident notification by providing timely information and reports as required by ~~policy or directives of~~ the office.

(c) (1) The office ~~shall~~ *may* conduct, or require to be conducted, an independent security assessment of every state agency, department, or office ~~at least once every two years.~~. The cost of the independent security assessment shall be funded by the state agency, department, or office being assessed. ~~The independent security assessment shall include, to the extent practicable, all of the following components and shall be conducted in compliance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Controls:~~

~~(A) Vulnerability scanning, that includes, but is not limited to, all of the following:~~

~~(i) Validation that IT systems have currently supported software, with all necessary security patches and updates applied.~~

~~(ii) Validation that system security configurations are in compliance with NIST standards.~~

~~(iii) Validation that the network architecture is arranged so as to separate internal, publicly accessible, and external zones, along with a mechanism to identify and alert on attempted intrusions.~~

~~(B) Penetration testing, when determined appropriate by the Office of Emergency Services.~~

~~(C) A report on the number, severity, and nature of identified vulnerabilities and recommendations for remediation and risk mitigation.~~

~~(2) (A) The Military Department may perform an independent security assessment required by paragraph (1).~~

~~(B) The Military Department may mitigate the impact of a cyber attack or assist a law enforcement investigation into cyber security upon the request of the Office of Emergency Services, a state law enforcement agency, or a state agency, department, or office.~~

~~(C) The Military Department may perform a cyber security assessment or respond to a cyber security incident impacting state infrastructure upon the request of the Office of Emergency Services.~~

~~(d) The Department of Technology may require a state agency, department, or office to redirect any funds within its budget that may be legally expended for these purposes, to pay the costs of becoming compliant with any recommendation made in an independent security assessment.~~

~~(e)~~

(2) In addition to the independent security assessments authorized by paragraph (1), the office, in consultation with the Office of Emergency Services, shall perform all the following duties:

(A) Annually require no fewer than thirty-five (35) state entities to perform an independent security assessment, the cost of which shall be funded by the state agency, department, or office being assessed.

(B) Determine criteria and rank state entities based on an information security risk index that may include, but not be limited to, analysis of the relative amount of the following factors within state agencies:

(i) Personally identifiable information protected by law.

(ii) Health information protected by law.

(iii) Confidential financial data.

(iv) Self-certification of compliance and indicators of unreported noncompliance with security provisions in the following areas:

(I) Information asset management.

(II) Risk management.

(III) Information security program management.

(IV) Information security incident management.

(V) Technology recovery planning.

(C) Determine the basic standards of services to be performed as part of independent security assessments required by this subdivision.

(3) The Military Department may perform an independent security assessment of any state agency, department, or office, the cost of which shall be funded by the state agency, department, or office being assessed.

(d) ~~(1) The office, Military Department, or entity~~ *State agencies and entities* required to conduct *or receive* an independent security assessment pursuant to subdivision (c) shall transmit the *complete* results of that assessment ~~only to the state agency, department, or office that was the subject of that assessment~~. *and recommendations for mitigating system vulnerabilities, if any, to the office and the Office of Emergency Services.*

(e) The office shall report to the Department of Technology and the Office of Emergency Services any state entity found to be noncompliant with information security program requirements.

~~(2) The office, Military Department, or entity required to conduct an independent security assessment pursuant to subdivision (c) shall transmit an aggregate of the results of that assessment to the Department of Technology.~~

~~(3) The Department of Technology shall adopt standards, to be included within the State Administrative Manual, setting forth the requirements for the office, Military Department, or entity required to conduct an independent security assessment pursuant to subdivision (c) to transmit, pursuant to paragraph (2), the aggregate of the results of that assessment to the Department of Technology, including, but not limited to, all of the following:~~

~~(A) Aggregated, statistical information relevant to the assessment results, including, but not limited to, the number of identified vulnerabilities categorized by high, medium, and low~~

~~risk. These results shall not include any specific information relative to the nature of the risk that is potentially exploitable.~~

~~(B) Prioritization of vulnerabilities.~~

~~(C) Identification of relevant internal resources.~~

~~(D) Strategy for addressing and mitigating those vulnerabilities.~~

(f) (1) ~~Transmission or communication of the results of an independent security assessment performed pursuant to subdivision (c) and any related information shall be restricted to~~*Notwithstanding any other law, during the process of conducting an independent security assessment pursuant to subdivision (c), information and records concerning the independent security assessment are confidential and shall not be disclosed, except that the information and records may be transmitted to* state ~~government~~ employees and state contractors who have been approved as necessary to receive ~~this~~ *the* information ~~in order~~ *and records* to perform that *independent security* assessment ~~by the office, Military Department, or entity required to conduct the independent security assessment.~~*, subsequent remediation activity, or monitoring of remediation activity.*

(2) The results of ~~an~~ *a completed* independent security assessment performed pursuant to subdivision (c), ~~the aggregate of the results of an independent security assessment transmitted to the Department of Technology pursuant to subdivision (e),~~ and any related information shall be subject to all disclosure and confidentiality provisions pursuant to any state law, including, but not limited to, the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1), including, but not limited to, Section 6254.19.

~~(3) Data produced during the creation of an independent security assessment performed pursuant to subdivision (c) shall be destroyed within one year of its date of creation, unless the Office of Emergency Services determines that retention for a longer period of time is necessary for state security.~~

(g) The office may conduct or require to be conducted an audit of information security to ensure program compliance, the cost of which shall be funded by the state agency, department, or office being audited.

(h) The office shall notify the Office of Emergency Services, Department of the California Highway Patrol, and the Department of Justice regarding any criminal or alleged criminal cyber activity

affecting any state entity or critical infrastructure of state government.

SEC. 2. The Legislature finds and declares that Section 1 of this act, which amends Section 11549.3 of the Government Code, imposes a limitation on the public's right of access to the meetings of public bodies or the writings of public officials and agencies within the meaning of Section 3 of Article I of the California Constitution. Pursuant to that constitutional provision, the Legislature makes the following findings to demonstrate the interest protected by this limitation and the need for protecting that interest:

The state has a very strong interest in protecting its information technology systems from intrusion, because those systems contain confidential information and play a critical role in the performance of the duties of state government. Thus, information regarding the specific vulnerabilities of those systems must be protected to preclude use of that information to facilitate attacks on those systems.

O